

CLAIMS

1. A method of providing a dynamic security management in an apparatus (1) comprising: a platform for running an application (2); a security manager (7) for handling access of the application (2) to functions (3) existing in the apparatus; an application interface (11A) between the platform and the application (2); a set of access permissions stored in the apparatus and used by the security manager (7) for controlling access of the application (2) to functions (3) through the application interface (11A), **characterised** by the steps of:
 - 10 downloading into the apparatus (1) an object containing access permissions applicable to at least one function (3);
 - verifying the object;
 - installing the access permissions together with the existing permissions.
- 15 2. A method according to claim 1, **characterised** in that the object is verified by checking a certificate chain of the object.
3. A method according to claim 1 or 2, **characterised** in that it is verified that a policy (8) of the function allows updates.
- 20 4. A method according to any one of the previous claims, **characterised** by downloading a further object containing a library (12), or the downloaded object further containing a library (12), said library (12) comprising new routines and/or new functions to be called by an application or library stored in the apparatus; and installing the library (12) to enable access of functions
25 (3) through the application interface (11A).
5. A method according to claim 4, **characterised** in that the new routines and/or new functions can access existing functions through a library (12).
- 30 6. A method according to claim 5, **characterised** in that the security manger (7), when accessing functions, recursively checks the permissions of the application interfaces (11A, 11B) and libraries (12) in a linked chain related to the called functions (3).
- 35 7. A method according to any one of the previous claims, **characterised** by downloading a further object containing an application (2), or the downloaded object further containing an application (2), said application (2) containing at least one new function; and installing the new function so that the new

function can access existing functions through the application interface (11A).

8. A method according to claim 7, **characterised** in that the new functions can access existing functions through a library (12).
- 5 9. A method according to any one of the previous claims, **characterised** in that the access permissions are contained in a policy file.
- 10 10. A method according to claim 9, **characterised** in that the policy file has a structure linking access levels of existing functions with a domain associated with the downloaded object.
- 15 11. A method according to claim 9 or 10, **characterised** in that the policy file has a structure linking access levels of existing functions with information contained in a certificate chain.
- 20 12. A method according to claim 11, **characterised** in that the information includes signature of the end entity certificate, signature of an intermediate certificate, or specific level information (level OID).
- 25 13. A method according to claim 10 or 11, **characterised** in that the policy file has a structure including logical expressions.
- 30 14. A method of providing a dynamic security management in an apparatus (1) comprising: a platform for running an application (2); a security manager (7) for handling access of the application (2) to functions (3) existing in the apparatus; an application interface (11A) between the platform and the application (2); a set of access permissions stored in the apparatus and used by the security manager (7) for controlling access of the application (2) to functions (3) through the application interface (11A), **characterised** by the steps of:
storing the access permissions in a security policy (8);
providing the security policy (8) with a hierarchical structure.
- 35 15. A method according to claim 14, **characterised** in that the security policy (8) has a structure linking access levels of existing functions with a domain associated with the downloaded object.
16. A method according to claim 15, **characterised** in that the security policy (8)

has a structure linking access levels of existing functions with information contained in a certificate chain.

17. A method according to claim 16, **characterised** in that the information includes signature of the end entity certificate, signature of an intermediate certificate, or specific level information (level OID).
18. An apparatus (1) with dynamic security management comprising: a platform for running an application (2); a security manager (7) for handling access of the application (2) to functions (3) existing in the apparatus (1); an application interface (11A) between the platform and the application (2); a set of access permissions stored in the apparatus and used by the security manager (7) for controlling access of the application (2) to functions (3) through the application interface (11A), **characterised** in that:
the apparatus (1) is arranged to download an object containing access permissions applicable to at least one function (3);
to verify the object; and
to install the access permissions together with the existing permissions.
19. An apparatus according to claim 18, **characterised** in that the security manager (7) is adapted to verify the object by checking a certificate chain of the object.
20. An apparatus according to claim 18 or 19, **characterised** in that the security manager (7) is adapted to verify that a policy of the function allows updates.
21. An apparatus according to any one of claims 18 to 20, **characterised** in that the apparatus is arranged to download a further object containing a library (12), or the downloaded object further containing a library (12), said library (12) comprising new routines and/or new functions to be called by an application (2) or library (12) stored in the apparatus; and to install the library (12) to enable access of functions through the application interface (11A).
22. An apparatus according to claim 21, **characterised** in that the new routines and/or new functions can access existing functions through a library (12).
23. An apparatus according to claim 22, **characterised** in that the security manager (7), when accessing functions, is adapted to recursively check the permissions of the application interfaces (11A, 11B) and libraries (12) in a linked chain

related to the called functions

24. An apparatus according to any one claims 18 to 23, **characterised** in that the apparatus is arranged to download a further object containing an application (2), or the downloaded object further containing an application (2), said application (2) containing at least one new function; and to install the new function so that the new function can access existing functions through the application interface (11A).
25. An apparatus according to claim 24, **characterised** in that the new functions can access existing functions through a library (12).
26. An apparatus according to any one of claims 18 to 25, **characterised** in that the access permissions are contained in a policy file.
27. An apparatus according to claim 26, **characterised** in that the policy file has a structure linking access levels of existing functions with a domain associated with the downloaded object.
28. An apparatus according to claim 26 or 27, **characterised** in that the policy file has a structure linking access levels of existing functions with information contained in a certificate chain.
29. An apparatus according to claim 28, **characterised** in that the information includes signature of the end entity certificate, signature of an intermediate certificate, or specific level information (level OID).
30. An apparatus according to claim 28 or 29, **characterised** in that the policy file has a structure including logical expressions.
31. An apparatus (1) of providing a dynamic security management in an apparatus comprising: a platform for running an application (2); a security manager (7) for handling access of the application (2) to functions (3) existing in the apparatus; an application interface (11A) between the platform and the application (2); a set of access permissions stored in the apparatus and used by the security manager (7) for controlling access of the application (2) to functions (3) through the application interface (11A), **characterised** in that the apparatus is arranged to:
store the access permissions in a security policy (8);

provide the security policy (8) with a hierarchical structure.

- 5 32. An apparatus according to claim 31, **characterised** in that the security policy (8) has a structure linking access levels of existing functions with a domain associated with the downloaded object.
- 10 33. An apparatus according to claim 32, **characterised** in that the security policy (8) has a structure linking access levels of existing functions with information contained in a certificate chain.
34. An apparatus according to claim 33, **characterised** in that the information includes signature of the end entity certificate, signature of an intermediate certificate, or specific level information (level OID).
- 15 35. An apparatus according to any one of claims 18 to 34, **characterised** in that the apparatus (1) is a portable telephone, a pager, a communicator, a smart phone, or an electronic organiser.